IL "PAESE INTERNET" NELLA SOCIETÀ DEL RISCHIO

Massimiliano Cannata
Maria Sabina Guerra
Rocco Mammoliti

La rete ha ormai raggiunto una dimensione pervasiva, diventando un eccezionale mezzo di trasmissione di dati, ma anche un veicolo di potenziali minacce, rispetto alle quali occorre organizzare un sistema di difesa adeguato, reattivo e con le necessarie competenze tecnologiche, in cui il fattore umano risulta essenziale. L'articolo, dopo una breve analisi dei trend di mercato e del modello di *Security Governance*, prende in esame la delicata funzione dei *Security Operation Center* nel monitoraggio e nella prevenzione del rischio informatico.

3.4

1. INTRODUZIONE

"*È a rischio la libertà del Paese Internet. Di fronte alla minaccia informatica il regno delle libertà, rappresentato dalla Rete, potrebbe esaurirsi di colpo*". Il grido d'allarme lanciato da Hannu Kari, docente presso l'Università della Tecnologia di Helsinki, attento studioso del mondo digitale, fotografa con efficacia l'"altra" faccia del progresso tecnologico. Si tratta solo di una tra le voci più celebri, attualmente impegnate ad analizzare l'evoluzione di quella sottilissima linea di confine che separa libertà e sicurezza. Un terreno difficile da definire, attorno a cui si sta giocando una partita delicatissima per il futuro della democrazia in molti Paesi.

Lo sviluppo dell'ICT ha indiscutibilmente segnato l'epoca che stiamo vivendo, alimentando la "quarta rivoluzione" industriale, che ha avuto nella rete un paradigma indiscusso di riferimento. *Velocità, interconnessione, immaterialità* [1] sono le categorie *dell'Information Society*, con cui siamo quotidianamente chiamati a rapportarci. La potenzialità di strumenti e apparati della tecnosociety appare sempre più evidente e va di pari passo al disvelamento di un'ineluttabile fragilità intrinseca, che si annida nella gestione e nell'implementazione delle reti digitali, le quali trasportano dati e informazioni e costituiscono il "sistema nervoso", che irrora l'economia di tutto il pianeta [2]. Fatti gravi ed eclatanti come quelli accaduti a New York, Madrid e Londra, i ripetuti black out verificatesi in molte regioni del globo, sono state "spie" eloquenti che hanno fatto emergere la dimensione globale del rischio [3], rendendo esplicita una prepotente e diffusa domanda sociale di sicurezza, che era rimasta allo stato latente nella parte finale del "secolo breve". *Nell'epoca del terrorismo* - ha scritto Kevin D. Mitnick, considerato l'hacker più famoso del mondo - *per proteggere le infrastrutture complesse non si potrà lavorare limitandosi a tappare delle falle, sarebbe come applicare una cultura da età della pietra ad un contesto socio economico segnato dal grande sviluppo della scienza e dalla rilevanza strategica del capitale intellettuale* [4].

"Difesa avanzata" sarà, infatti, la parola chiave con cui bisognerà misurarsi. Significa in concreto

delimitare in un circuito definito una "Dmz", che nel gergo militare designa la "*zona demilitarizzata dell'azienda*", individuabile in quelle superfici di contatto che separano l'organizzazione dal mondo esterno: dal portale internet ai server di posta, che sono porte d'accesso appetibili per chi vuole introdursi illecitamente nel perimetro interno di ogni realtà produttiva. Di fronte ai nuovi pericoli insiti nel contesto tecnologico le *Corporation* stanno cercando di dotarsi di un'architettura di rete che protegga le informazioni riservate e le aree a più stretto contatto con il business, dando corpo ad una sorta di "seconda rete", un meta livello blindato, che dovrà essere fuori dalla portata di qualsiasi genere di insidie: dalle frodi, allo spionaggio industriale, alla sottrazione illecita di informazioni sensibili. Nella dimensione ormai dominante della globalizzazione, costruita su sistemi industriali aperti e interconnessi, la sicurezza non è più concepibile come semplice *commodity*, la cui qualità può risultare valutabile solo in relazione alle performance di ogni singola applicazione, sarà piuttosto percepita come un valore per il business, oltre ad un importante fattore abilitante dell'innovazione.

2. TREND DI MERCATO

Il paradigma della rete, al quale si è fatto riferimento nel paragrafo introduttivo, è il termine di collegamento essenziale per capire il nesso che lega lo sviluppo dell'*Information Society* e la nuova prospettiva della **sicurezza**. Internet, tecnologie e business sono fattori sempre più legati. Secondo uno studio dell'IDC [5] nell'universo delle aziende italiane che hanno più di dieci dipendenti, l'88% utilizza internet, il 70% ha una presenza sul web, il 25% si serve di una linea intranet /extranet, mentre il 50% degli addetti dotati di PC risulta costantemente connesso. I dati confermano il processo di profonda mutazione tuttora in atto, in cui internet è soltanto uno dei vettori di trasporto più noti, che si interseca in un mondo intangibile, e nello stesso tempo reale, che ha estremo bisogno di un governo costante della sicurezza. Gli interrogativi dei ricercatori riguardano la possibilità di difendere un contesto, come quello ICT, che vede 155 milioni di nuovi utenti nel 2006 e che si prevede potrà avere nei prossimi quattro anni, due miliardi di utenti mobili e due miliardi di utenze broadband. Il mercato della sicurezza, secondo le stime elaborate da Assinform [6], ha superato i diciotto miliardi di dollari, con un tasso di crescita pari al 15-18% annuo. L'ammontare dei danni [7] per incidenti è pari a cinquanta miliardi di dollari con un tasso di crescita de 45%. Anche i dati che riguardano il mercato italiano confermano i trend di crescita del fenomeno. Nel 2006 il business di questo comparto ha superato gli 800 milioni di euro, con un incremento che nel biennio 2004-2006 è stato del 70%. Nessun altro ambito dell'*Information Technology* ha mostrato performance così positive. Non crescono unicamente i volumi di spesa. Si avverte, infatti, nelle grandi organizzazioni, l'esigenza di aumentare il perimetro di responsabilità dei manager del settore. La moltiplicazione delle minacce è un dato critico contro cui aziende e istituzioni stanno cercando di correre ai ripari. Secondo uno studio della *Morgan Stanley*, la priorità per i responsabili dei Sistemi Informativi delle aziende che figurano nella prestigiosa classifica *Fortune 1000*, è proprio la sicurezza. Il volume degli investimenti in sistemi di protezione (stimati dall'ultimo Rapporto Assinform in 585 milioni di euro) – (Figura 1) rappresenta il 3% dell'intero budget dell'*Information Technology*. Una performance ancora piuttosto bassa se

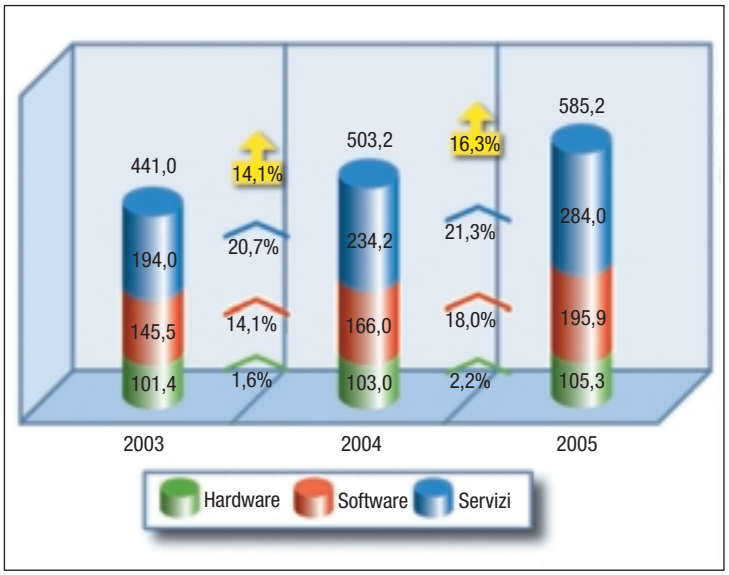

FIGURA 1

Gli investimenti IT in Italia nel periodo 2003/2005 (valori in milioni di euro - variazioni in percentuale). Fonte: Aitech-Assinform/NetConsulting

si considera che a livello internazionale questo comparto occupa l'11% dell'intero settore IT. Al di là delle molteplici chiavi di lettura, alcuni indicatori sono comunque da leggere in positivo, come l'aumento del numero delle aziende che dedicano risorse per tutelare il proprio business e la generale crescita delle organizzazioni industriali, che stanno impegnando energie e competenze nell'elaborazione di policy e strumenti di controllo del crimine informatico.
Le forme di attacco e di intrusione si stanno evolvendo allo stesso ritmo del progresso tecnologico. La diffusione di sistemi mobili e di apparati di connessione cellulare – computer, associati ad un elevato uso della rete hanno generato dei momenti di contatto tra le aziende e l'ambiente esterno, con un inevitabile aumento dei fattori di esposizione e di rischio [8]. La scomparsa di un "perimetro" lavorativo tradizionalmente definito, ha reso molto più labile l'idea di confine, obbligando le organizzazioni produttive a ripensare i criteri e gli strumenti attraverso cui si attuano le strategie della sicurezza fisica e informatica. In quest'ottica è possibile spiegare il flusso crescente di investimenti, che salta facilmente all'occhio osservando le statistiche e gli studi di settore.

3. IL MODELLO DI SECURITY GOVERNANCE

Nel settore dei servizi e delle telecomunicazioni, l'infrastruttura ICT presenta un carattere pervasivo, rilevante e complesso. Bisogna partire da questo elemento oggettivo per capire il ruolo che riveste la sicurezza informatica in termini di pianificazione, progettazione, gestione operativa. Il primo dato che va preso in considerazione riguarda l'applicazione sempre più capillare delle policy aziendali, che affiancata da una decisiva azione di contenimento e contrasto delle diverse metodologie di attacco, consente di determinare un'apprezzabile riduzione della tempistica di previsione e individuazione delle diverse tipologie di minacce, anche di quelle non convenzionali, che corrono sui binari digitali. La variabile tempo è oggi un *must* essenziale con cui il *security manager* deve misurarsi e su cui è chiamato a dare risposte immediate.
Il modello di gestione della sicurezza utilizzato si basa su tre processi ciclici tra loro correlati: *prevenzione, gestione incidenti, gestione crisi* (Figura 2).
Le attività di contrasto prevedono l'attuazione di azioni finalizzate a contenere i danni provocati dall'incidente informatico, il corretto ripristino dei processi di business critical, l'analisi delle evidenze e degli impatti verifi-

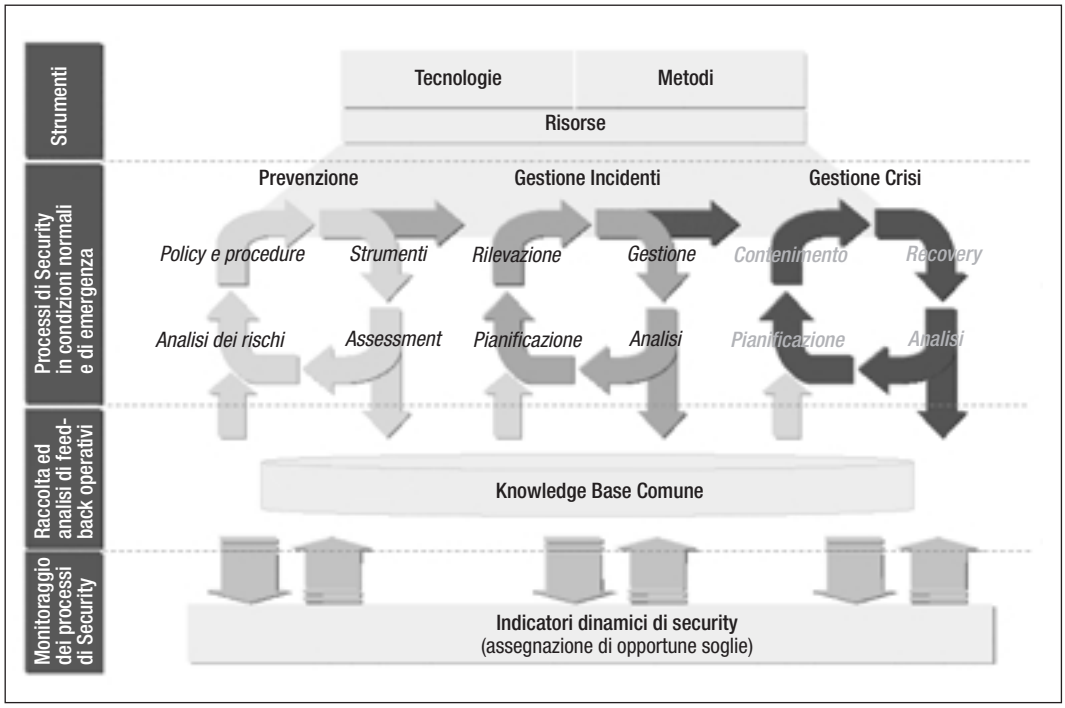

FIGURA 2
Modello di gestione della sicurezza

catisi, e infine la pianificazione di una strategia volta a prevenire ulteriori crisi. Bisogna fare i conti per ottenere dei risultati con due fenomeni mutuati dalle scienze biologiche: l'immunizzazione e l'adattamento [9]. Rispetto agli attacchi che provengono dal mondo esterno, il soggetto – impresa cerca di mettere in moto nel più breve tempo possibile gli anticorpi per assicurarsi la sopravvivenza.
Non bisogna dimenticare che i processi di information security nel contesto della società complessa devono essere supportati da un complesso di tecnologie, metodi e risorse dedicate. In ogni organizzazione le informazioni prodotte a seguito delle attività svolte devono alimentare una *knowledge base* comune, una sorta di *koinè* che renda decodificabili codici e linguaggi, da utilizzare come *database* degli incidenti gestiti. Tale corpus aggiornato di dati consente di sviluppare analisi complesse, (di tipo economico, statistico, informatico, tecnologico) diventando il supporto per la gestione di possibili futuri incidenti. La *knowledge base* è il deposito prezioso da cui si ottengono alcuni indicatori di sintesi, che forniscono una valutazione in tempo reale dello stato di sicurezza degli *asset* aziendali.

4. I SECURITY OPERATION CENTER

Per abbassare la soglia di vulnerabilità, ormai intrinseca ad ogni sistema telematico e per sviluppare al meglio le attività di identificazione, monitoraggio e rilevazione delle aggressioni informatiche, Telecom Italia ha dato vita ad un progetto innovativo che si è concretizzato nella creazione e gestione integrata del SOC (*Security Operation Center*). Questa struttura impegna *analisti specializzati* nel monitoraggio degli strumenti di sicurezza, nella gestione degli incidenti informatici e nell'erogazione dei servizi di sicurezza IT [10]. Le attività svolte dal SOC sono riassumibili in cinque macro-aree. *Security Assessment*, finalizzato alla verifica dei livelli di protezione presenti sui sistemi di Information Technology e sulle applicazioni; *Security Monitoring* che si sviluppa nella individuazione degli eventi anomali e potenzialmente pericolosi per i sistemi e le infrastrutture aziendali. *Incident Handling*, termine che definisce il coordinamento delle strutture di esercizio coinvolte negli incidenti di sicurezza e il mantenimento del presidio di controllo fino alla completa evoluzione dei fenomeni critici. Le azioni di *Security Software e Security Communication* completano la mappa di un particolare "*global-system*", in cui l'attenzione per il fattore tecnologico e per le diverse componenti culturali, entra a far parte di una complessa catena del valore. Nelle architetture del SOC i fattori di innovazione si traducono, infatti, in un progetto di *Governance*, orientato a sfruttare la legge dei "rendimenti crescenti" che trova la sua applicazione concreta nell'intelligenza collettiva" distribuita nelle reti digitali [11]. Per pensare in termini di valorizzazione del "network" i soggetti imprenditoriali sono sempre più sollecitati a condividere linguaggi, informazioni, metodologie e strumenti.
I diversi volti di un *Security Operation Center* possono essere riassunti in:
- una struttura tecnologica che garantisce la possibilità di centralizzare la gestione e di monitorare tutti i sistemi e gli strumenti di sicurezza aziendali;
- una struttura organizzativa che opera su base H24 per presidiare la sicurezza informatica, garantendo una maggiore rapidità di intervento in presenza di incidenti di natura informatica;
- un centro di competenza, costituito da personale specialistico in grado di elaborare ed analizzare le informazioni raccolte dagli strumenti tecnologici e di indirizzare le opportune azioni di contrasto e contenimento degli incidenti di sicurezza;
- un centro specialistico che eroga servizi di sicurezza verso le strutture interne ed esterne correlate.

Le attività di un SOC generano vantaggi su alcuni versanti critici, presentando degli impatti non trascurabili sulle attività operative. In particolare:
- la riduzione delle tempistiche di attuazione dei piani di sicurezza interni e delle direttive fornite dal top management;
- la riduzione dei livelli di rischio e, di conseguenza, dei danni economici o di immagine derivanti da incidenti o dalle crisi di natura informatica;
- la razionalizzazione e l'ottimizzazione degli investimenti in infrastrutture di sicurezza all'interno dell'organizzazione;

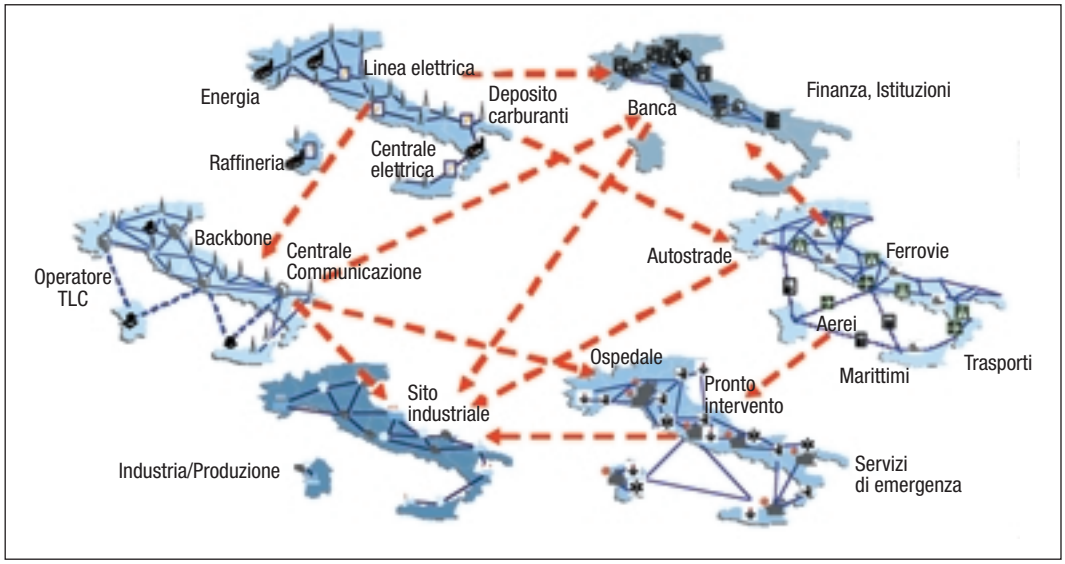

FIGURA 3
Interdipendenze tra infrastrutture critiche

❑ la costituzione di un centro di competenza nei riguardi dell'*Information Security*, capace di proporre servizi di sicurezza innovativi;
❑ il potenziamento e l'ottimizzazione delle skills tecnologiche.

L'interconnessione tra i SOC realizza un approccio collaborativo alla sicurezza informatica, complementare rispetto al metodo di tipo reattivo e proattivo, elaborato da ogni singola struttura. Condividere le informazioni inerenti agli incidenti, le linee di azione da intraprendere per contrastare gli attacchi, le metodologie di analisi e prevenzione, creare protocolli comuni di comunicazione, definire set di strumenti avanzati per erogare servizi utili nelle situazioni di crisi, sono obiettivi che richiedono un costante contatto tra i centri di elaborazione dati, distribuiti sul territorio. La connessione tra i diversi SOC consente una più efficace attività di prevenzione e contrasto agli incidenti, intrusioni e infezioni. La diminuzione costante della vulnerabilità, che Telecom Italia ha registrato nell'ultimo anno, ha consentito di scongiurare i danni economici e di immagine derivanti da azioni illecite e dalle violazioni dei sistemi informatici. Il risultato positivo è stato ancora più forte se si considera il vantaggio in termini di efficienza, generato dal contenimento dei disservizi, imputabili ad attacchi particolarmente sofisticati portati al cuore delle infrastrutture critiche (Figura 3). Allo stato attuale esistono, nello scenario italiano, impianti assimilabili ai SOC che non possiedono presidi e strumenti adatti a favorire lo scambio e il dialogo, con un duplice svantaggio rappresentato dallo sfruttamento parziale delle risorse e da una generale sovraesposizione alle potenziali minacce di tipo informatico delle reti di comunicazione che sono di vitale importanza per il nostro sistema – Paese.

Tutti i SOC, per le ragioni precedentemente esposte, possono trarre vantaggio dalla creazione di un network (Figura 4). Le strutture che hanno pochi strumenti a disposizione possono infatti giovarsi dell'apporto di presidi ICT avanzati, ottenendo un significativo potenziamento delle capacità di governo della sicurezza. Questo flusso collaborativo oltre a colmare i gap informativi, può ridurre il rischio che i SOC, che definiamo a questo punto per comodità "minori", una volta infettati, diventino mezzo di trasporto e diffusione di attacchi informatici sulla rete.

Nell'ottica di sviluppare una "rete allargata di collaborazione", Telecom Italia ha, poi, individuato tre livelli di condivisione: nel primo vengono considerate le informazioni di sicurezza, nel secondo le metodologie, nel terzo gli strumenti.

4.1. Condivisione delle informazioni

La condivisione delle informazioni (Figura 5) nasce come frutto delle attività dei singoli SOC, in relazione a:

❑ gli incidenti rilevati;
❑ la diffusione di nuovi virus/worm;
❑ la scoperta di nuove vulnerabilità;
❑ *l'Intelligence Analysis* di attacchi informatici.

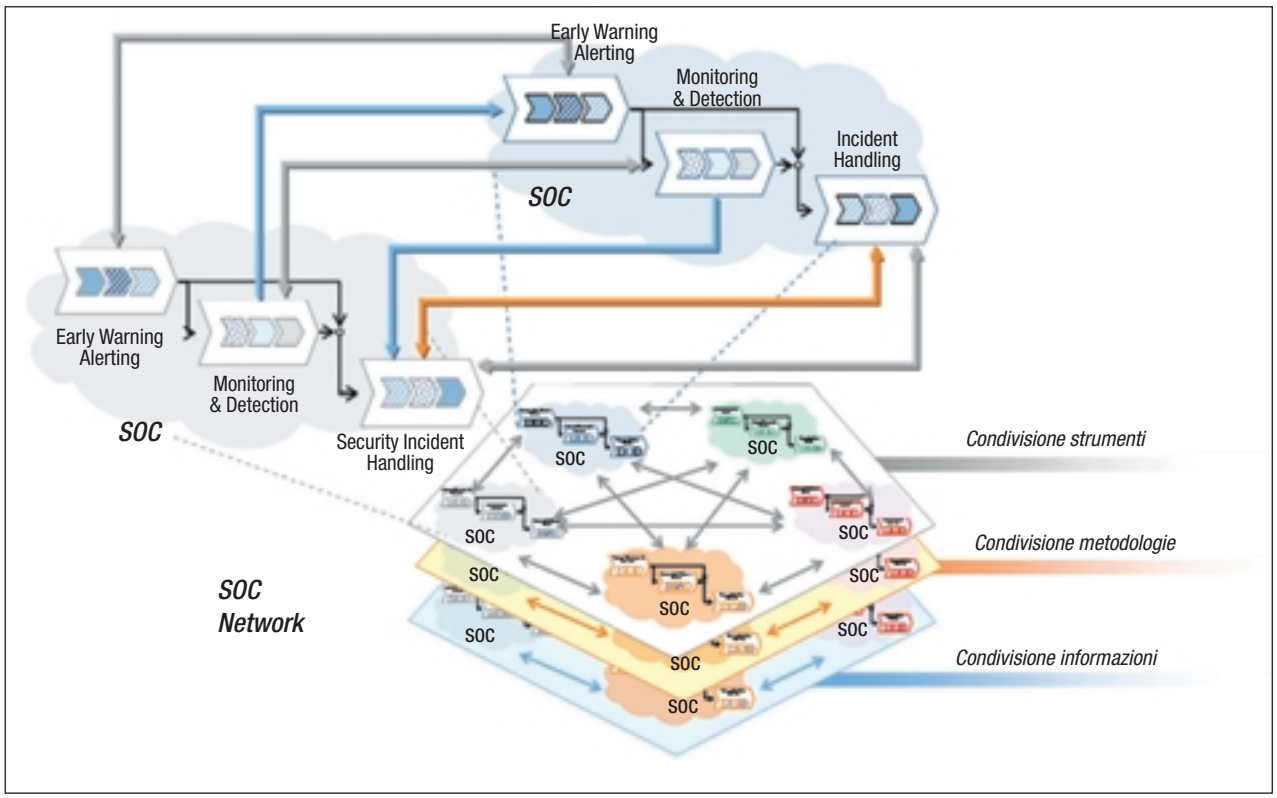

FIGURA 4

Modello di SOC Network

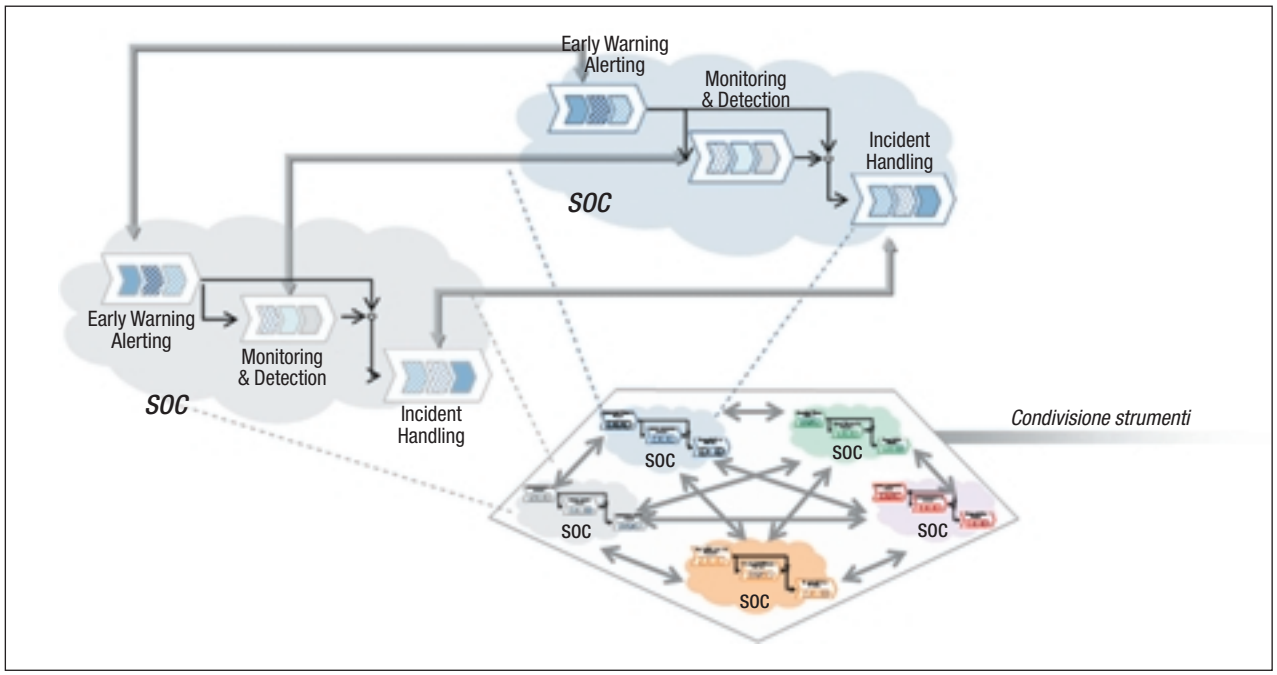

FIGURA 5

Primo livello di networked SOC

In questo primo livello di collaborazione è possibile registrare un generale rafforzamento del livello di consapevolezza di tutto il personale impegnato su tematiche di security, con un riflesso sul miglioramento delle attività di prevention ed un incremento sulla tempestività delle azioni di contrasto, di contenimento e di ripristino dei siste-

mi, a seguito di ogni attacco informatico.
Come mostra la figura 5, la "*SOC networked*" condivide l'output generato dalle attività di *Security Early Warning Alerting*, implementate da ogni singolo SOC. Il dato finale di sintesi delle attività del SOC è molto chiaro: l'incidente è stato rilevato, analizzato e, nei casi in cui è possibile, gestito.
Analizzando le informazioni riguardo agli incidenti di sicurezza registrati è possibile verificare se la rete aziendale presenta delle vulnerabilità che la rendono potenzialmente soggetta a determinate tipologie di attacco e, in caso positivo, pianificare in tempo utile le strategie di intervento prima ancora che gli eventi si manifestino. Un valore aggiunto è costituito dalla opportunità di beneficiare degli output delle tecnologie in dotazione a tutti gli impianti. Un esempio è rappresentato uno strumento di *Anomaly Detection*, non presente nella rete commerciale, oggi in dotazione, in via sperimentale, solamente a queste speciali strutture. Con l'*Anomaly Detection* vengono rilevati malware ancora sconosciuti, non identificabili attraverso gli strumenti tradizionali che tecnicamente vengono denominati *signature-based*, di cui fanno parte gli IDS. Il SOC, che usufruisce della rete collaborativa, divulgherà l'identificazione del nuovo *malware* a tutte le altre strutture analoghe, che potranno beneficiare uniformemente delle potenzialità innovative dell'applicativo, con un risparmio di risorse e un innalzamento della qualità delle performance.
La scoperta e la divulgazione ai SOC di nuove aree critiche esposte al rischio, permettono di prevenire infezioni o intrusioni. Un caso molto diffuso è dato dalla scoperta di una vulnerabilità accessibile dal web che può, in qualche caso portare, al *defacement* del sito. Il processo che si innesca ha una precisa cadenza: quando si verifica questa tipologia di attacco il network, e non una singola struttura, si incarica di comunicare la vulnerabilità, evitando, così che la stessa debolezza possa essere sfruttata per modificare le interfacce Internet di tutta l'azienda.
Infine la condivisione di informazioni provenienti dalle attività di *intelligence* dei singoli SOC risulta particolarmente utile per far fronte comune a violazioni informatiche che vanno dallo spionaggio industriale agli attacchi di tipo terroristico. Questo protocollo di difesa determina un innalzamento del grado di sicurezza complessivo: nel momento in cui una singola struttura individua e segnala un incidente, tutti gli altri attori della "rete collaborativa" ne sono a conoscenza, con la possibilità di prevenire il diffondersi del *malware*.
Un ulteriore vantaggio che rientra nel paradigma adottato da Telecom Italia è riscontrabile sulle infezioni che si manifestano su larga scala. Tramite l'attività di prevenzione distribuita sul *SOC Networked* è possibile privare i *malware* del terreno fertile, indispensabile per la diffusione del fenomeno.

4.2. Condivisione delle metodologie

Il secondo livello di collaborazione presuppone un processo più avanzato di integrazione. Alla condivisione informativa, si sovrappone la condivisione delle metodologie (Figura 6) di analisi e di *Incident Handling* che definiscono i processi in base ai quali i SOC operano per fronteggiare e gestire un incidente.
Siamo ad un capitolo nuovo della sicurezza. Il flusso di scambio che intercorre tra i SOC non è più limitato alle informazioni prodotte dai processi interni. L'uso di metodologie comuni consente, infatti, di innestare con facilità le informazioni intermedie provenienti dai vari centri, parallelizzando il lavoro di analisi e velocizzando la convergenza del processo verso il risultato finale. Lo scambio di dati tra i diversi SOC non impatta solo sulle attività di *Security Communication*, ma anche sui passaggi intermedi, come nel caso dell'*Incident Handling*. L'uniformità di approccio metodologico significa in concreto, rendere commensurabili le diverse tecniche di intervento messe in atto dalle singole strutture che possono sfruttare il network collaborativo per elaborare una strategia condivisa di *Security Governance*.
L'adozione di metodologie, che giunge a vallo di uno scambio informativo, consente di reagire alle criticità senza aspettare la conclusione delle procedure di gestione degli attacchi, con un vantaggio notevole sul fattore tempo che, come abbiamo già visto, è uno dei punti critici su cui si misura la qualità degli interventi di messa in sicurezza degli asset intangibili delle imprese high – tech.

4.3. Condivisione degli strumenti

Richiede il grado più alto di collaborazione tra i SOC, perchè prevede una condivisione delle informazioni, delle metodologie e degli strumenti di sicurezza (Figura 7). Questo, che potremmo definire come un "meta livello" consente, in particolare, di:

- ❑ scambiare informazioni in qualsiasi punto della "catena del valore";
- ❑ fronteggiare e gestire i cosiddetti "picchi" nelle richieste di erogazione dei *security services*;
- ❑ contrastare in modo efficace attacchi informatici particolarmente pericolosi rivolti verso i perimetri delle reti presidiate;

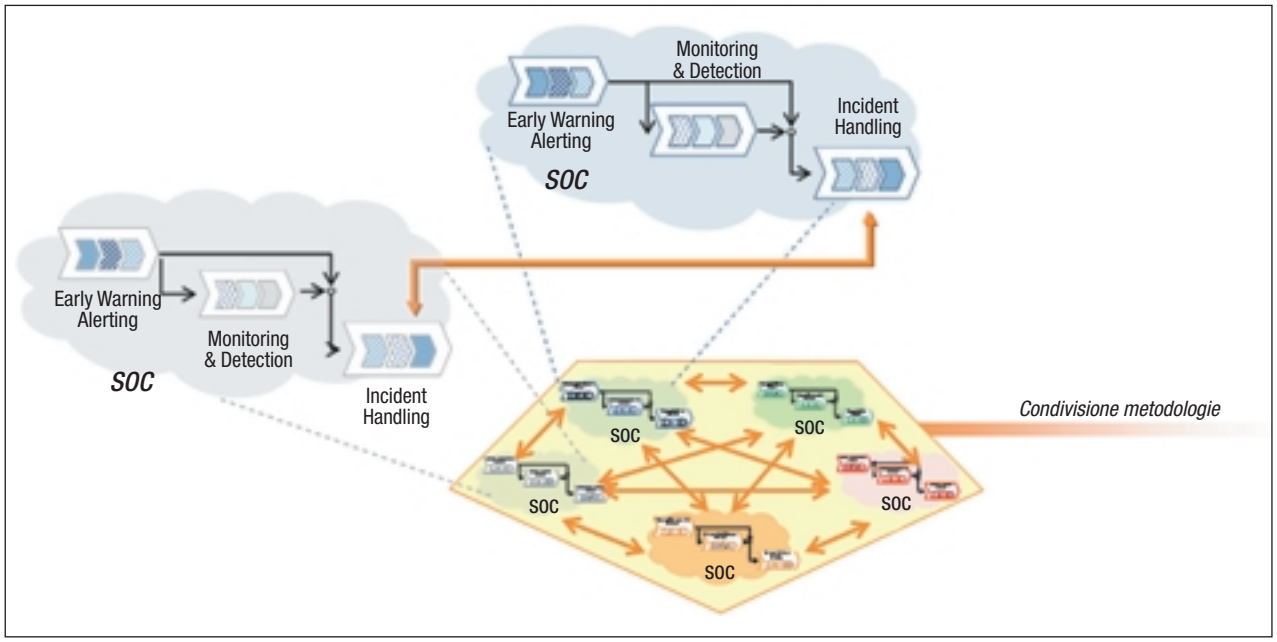

FIGURA 6

Secondo livello di networked SOC

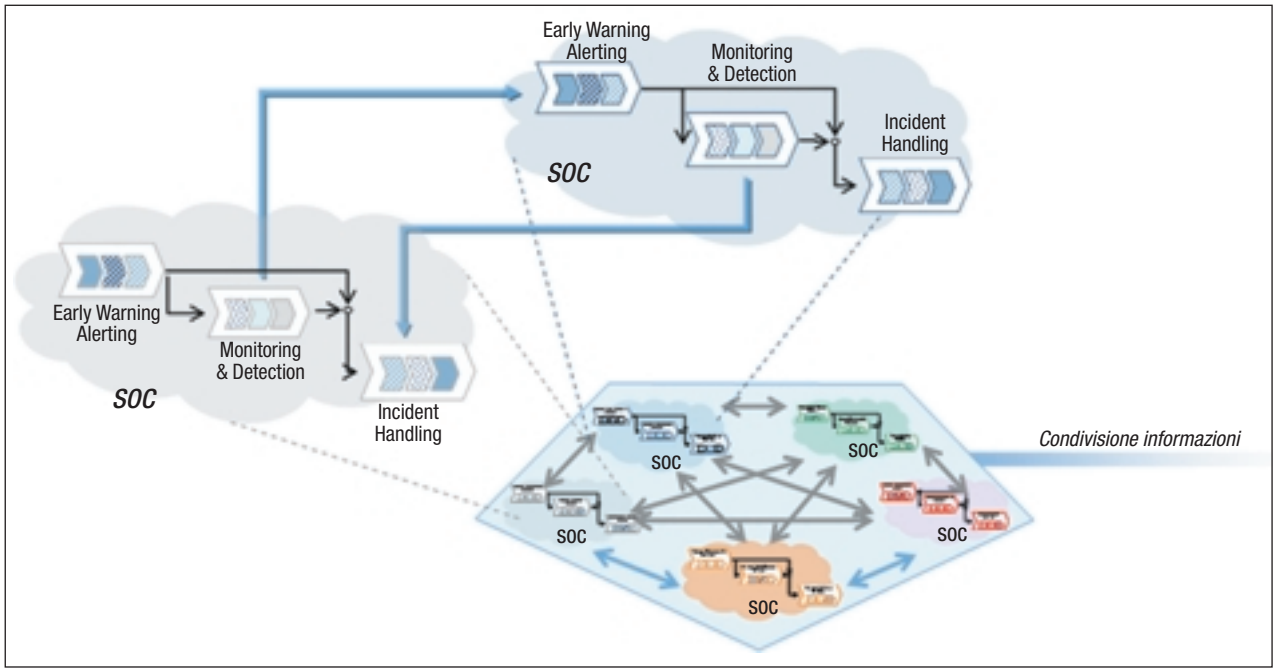

FIGURA 7

Terzo livello di networked SOC

❑ salvaguardare le infrastrutture informatiche di importanza nevralgica.

Lo scambio di informazioni può avvenire anche al più basso livello, significa in concreto che in ogni momento è possibile condividere l'output ancora non completamente elaborato da un singolo SOC, disponendo di dati parziali. Un esempio interessante è relativo all'utilizzazione degli strumenti di monitoraggio e di simulazione: all'interno del SOC si rilevano comportamenti sospetti, scatta quindi una simulazione che tenendo conto dei parametri che caratterizzano l'evento critico, ha lo scopo di studiare e stimare tutti i possibili effetti reali e le conseguenze per il business. Può essere ancora una volta interessante condividere i dati parziali prodotti dalle simulazioni; infatti, fornendo i parametri del comportamento sospetto alle strutture omologhe, queste possono ricostruire l'evento nel proprio contesto di rete, misurando con estrema precisione tutti gli effetti sulle attività di business, generate dall'*Early Warning* segnalato.

Da un punto di vista operativo, avendo strumenti e metodologie comuni, è possibile per Telecom Italia prendere in carico una quantità maggiore di *Security Services*. È, inoltre, ipotizzabile che nel caso in cui un singolo SOC non riesca ad evadere tutte le richieste di servizio che gli pervengono, possa attivare gli altri centri che operano sul territorio, con una maggiore soddisfazione di tutti i clienti e con un innalzamento del livello di sicurezza complessivo.

I SOC oltre alle informazioni finali che vanno ad alimentare i processi di *Security Alerting* e alla elaborazione dei passaggi critici intermedi (come per esempio l'*Incident Handling*), devono attivare un processo continuo di scambio delle informazioni interne, non trattate. Questo rende possibile l'effettuazione di analisi degli stessi dati in luoghi e strutture diverse, consentendo di verificare numeri e quantità finali. Il feedback di controllo che si ottiene ha un grande valore per le aree sensibili, perché implicitamente introduce un percorso di ridondanza delle segnalazioni, che riduce le probabilità di errata gestione dei dati a disposizione.

Il livello di condivisione degli strumenti, tra quelli analizzati, è sicuramente la soluzione più invasiva e dispendiosa che esprime anche il massimo grado di collaborazione tra i SOC. Il raggiungimento di uno scambio così fitto di dati e di informazioni rende, agli occhi di un osservatore esterno addirittura sfumata e perciò poco percepibile la differenza tra i vari livelli della Security Governance e dei SOC che operativamente traducono le strategie in policy di tutela e difesa del patrimonio immateriale dell'azienda. Tuttavia proprio da questo modello avanzato di integrazione e dal network collaborativo potrà scaturire un livello superiore di tempestività negli interventi e una più efficace prevenzione degli incidenti informatici, con un beneficio che non ha solamente un rilievo di tipo economico, ma un impatto di natura sociale certamente ampio e importante.

5. LE NUOVE SFIDE

La scelta di rafforzare l'azione di contrasto alle minacce informatiche verso le infrastrutture tecnologiche, tramite la creazione e la gestione integrata del SOC, si è tradotta per Telecom Italia in un grosso investimento delle risorse migliori, oggi impegnate a fronteggiare minacce tecnologicamente complesse, ma soprattutto a sviluppare capacità di contrasto rispetto ad un crimine senza volto, né territorio che sferra attacchi sofisticati, di cui è sempre più difficile capire: portata, conseguenze, pericolosità, sviluppi. Si evolvono le azioni illecite: intrusioni, frodi telematiche, insider, attacchi distribuiti. Queste forme di violenza, che non esitano a transitare sui binari digitali e sui new media nei casi più eclatanti hanno assunto le sembianze di reati di *competitive intelligence* e di spionaggio industriale, portate avanti da organizzazioni delinquenziali che mirano alla sottrazione di dati sensibili, che in molti casi rivestono un valore strategico.

La mappatura delle possibili vittime per un lavoro che, come abbiamo descritto, si svolge dentro e fuori dal tradizionale perimetro aziendale, è tanto complessa, quanto estesa: si va dagli utenti privati, ai singoli cittadini che sono potenziali vittime di virus, hacker e frodi on line, ai cosiddetti utenti qualificati (come le aziende) sempre più og-

getto delle attenzioni degli insider. Per gli utenti classificati infrastrutturali (come i ministeri, le istituzioni, le forze dell'ordine, le ambasciate ecc.) il pericolo proviene da molteplici fonti esterne, tra cui, come si ricordava prima, le organizzazioni terroristiche a livello internazionale.
Multifunzionalità, infrastruttura di rete, autenticazione, protezione dei sistemi di etichettatura e degli applicativi VOIP saranno nei prossimi anni al centro delle analisi degli studiosi in tutto il mondo.
Sul fronte della ricerca portata avanti dal mondo Telecom Italia, è necessario ricordare che per limitare la proliferazione di worm, virus e maleware è stato avviato il progetto "*Moses*", che ha aperto un confronto con tutto il mondo della progettazione delle SIM Card, che consentirà di mettere in campo terminali mobili, dotati di tecnologie adatti a minimizzare gli impatti di attacchi e azioni illecite e a garantire la continuità dei servizi ICT che corrono sulle infrastrutture critiche. Gli antivirus già presenti sul mercato risultano, infatti, inefficaci rispetto ad uno standard che deve prima di tutto scongiurare il *gap* di performance delle reti, che sono causa di perdite molto gravi per il business delle aziende e per il funzionamento delle istituzioni. Tra gli obiettivi a breve termine su cui stanno lavorando i ricercatori va ricordata la creazione di una *knowledge* informativa condivisa, destinata a svilupparsi in coerenza con la messa in esercizio di sistemi ad alto potenziale conoscitivo e con il rilascio sul mercato di soluzioni compatibili con la dimensione della personal *communication* [13].
La SIM card, il piccolo cuore elettronico dei nostri telefonini, per un azienda di servizi TLC, rappresenta un asset strategico. Data l'altissima disponibilità di terminali sempre più avanzati nell'universo digitale, diventerà cruciale l'identificazione degli attori di questo specifico cyber spazio. Tanti momenti essenziali della nostra vita di lavoro hanno ormai una traccia corrispondente in rete ed è facile comprendere quali conseguenze tutto questo potrà avere sul piano della sicurezza individuale e collettiva nella società del rischio. *Identity Access Management* è la parola chiave per un settore della ricerca destinato ad avere significativi e immediati sviluppi. In un domani, neanche troppo lontano, la nostra piccola SIM potrà servire a pagare i parcheggi, ad avere info sui trasporti, ad ordinare i film, a pagare il biglietto del cinema da casa, a partecipare a giochi e community. Avremo in mano una chiave elettronica, un *passpartout* intelligente che dovrà contenere un *security box* con i nostri dati sensibili. Scelte, interessi, gusti, preferenze, troveranno voce attraverso le reti, in un escalation che i player di tlc dovranno preoccuparsi di studiare e tutelare. Questa prospettiva che vede il telefonino tramutarsi in un terminale che servirà a gestire in connessione con piattaforme evolute, contenuti multimediali sempre più sofisticati, sarà caratterizzata da investimenti significativi destinati alla protezione dei dati e alla riservatezza delle comunicazioni.
Il prepotente sviluppo della larga banda, la progressiva pervasività dell'*Internet Protocol*, vanno a costituire una visione unitaria in cui l'orizzonte della ricerca sulle problematiche di *Security* si intreccia nel contesto articolato e dinamico caratterizzato dello sviluppo dei servizi a valore aggiunto (VAS). Si tenderà a privilegiare un rapporto di fiducia tra l'azienda e il cliente. L'impresa diventerà soggetto attivo: vivrà sempre più nella relazione con il suo pubblico, costruita sulla responsabilità e sull'affidabilità, in una dialettica di confronti che tenderà ad attribuire ai termini convergenza e competitività, significati sempre più ampi e trasversali. Gli operatori dovranno in questo processo dinamico e articolato, ancora allo stato nascente, imparare a soddisfare tre precise esigenze: la sicurezza nell'utilizzazione di reti e terminali; il rispetto dei diritti digitali al fine di scongiurare illegalità e sfruttamento indebito dei contenuti; la personalizzazione dello strumento che ormai dialoga tramite un'interfaccia semplice e immediata, con l'utente e si adatta, come una protesi, al suo linguaggio, ai suoi gusti e alle sue preferenze.
La connettività integrata della telefonia fissa e mobile verrà incontro a queste richieste rappresentando il cliente nell'eco-sistema dell'operatore, costruito sull'*Internet Protocol* che governa l'accesso ai terminali e ai

servizi nei più vari ambiti: dalla televisione, al commercio elettronico, dagli acquisti on line ai trasporti. Va sottolineato il passaggio da un *paradigma di autenticazione Username – Password*, che è quello maggiormente in uso nelle aziende, ad un paradigma *challenge – Response*, che significa assicurare una maggiore robustezza di autenticazione e trasparenza ai consumatori. Una risposta è già individuabile nei laboratori di Telecom Italia che stanno mettendo a punto interfacce radio a corto raggio che consentiranno all'utente di colloquiare, tramite le SIM, direttamente con gli oggetti dell'ambiente tecnologico, attivando uno scambio di dati e informazioni.

Ma la ricerca e l'innovazione impone anche dei ritmi di adeguamento sul fronte legislativo e normativo. L'entrata in vigore di policy mirate alla gestione delle informazioni sotto il profilo della riservatezza, a salvaguardare la sicurezza degli utenti e degli addetti alle strutture di *Information Technology*, colloca Telecom Italia sui più avanzati standard europei in materia di governance delle informazioni. Tali provvedimenti sono in sintonia con le recenti iniziative adottate dal Garante della Privacy, che hanno dato particolare enfasi alla tutela, nell'ambito delle organizzazioni aziendali, di tutti le forme di elaborazione, comunicazione e trasmissione del sapere e della conoscenza. Quella che a volte trattiamo superficialmente come un semplice mail, un documento di lavoro in Power Point, l'ultimo file di World, su cui abbiamo magari fatto annotazioni che possono rivestire un determinato livello di criticità, sono contenitori fragili di fatti riservati, in molti casi riconducibili a processi produttivi o ad azioni di rilievo strategico intraprese dai vertici, che è opportuno divulgare solo a destinatari ben definiti. In particolare la policy sulla gestione delle informazioni sotto il profilo della riservatezza disciplina aspetti particolarmente delicati, introducendo un criterio interpretativo capillare di classificazione dell'informazione secondo precise classi di rischio, in cui modernità normativa e innovazione tecnologica cammineranno sempre più vicine.

Infine un processo comune di ricerca che coinvolge le funzioni aziendali di Telecom Italia della *Business Continuity, Information Security*, ed *Employee Awareness* è in atto nel delicato settore delle frodi informatiche. Anche in questo ambito si tratterà di sviluppare in prima battuta una strategia efficace di prevenzione del fenomeno, per poi agire in sede di denuncia e di contrasto. La catena del valore aziendale comprende tutte le fasi di acquisizione, ingegnerizzazione e di sviluppo del servizio, fino al rilascio e alla gestione del cliente finale. Ad ogni passaggio corrisponde un indicatore corrispondente del rischio, che consente di misurare il livello del fenomeno e di escogitare le azioni adatte a prevenire i comportamenti fraudolenti. L'azione del management si sta concentrando su tutto il sistema dell'offerta, prendendo in esame tutte le tappe di sviluppo che implementano le offerte: dal mondo del "prepagato", al mondo dati per la telefonia fissa e mobile, ai VAS. Vari casi sono allo studio. Per esempio, spiegano i ricercatori, il momento di fine credito relativo alle utenze che corrono sulla telefonia di ultima generazione. L'analisi dei dati dalla erogazione iniziale del servizio, alla fase di *billing* (di pagamento) ha fatto emergere fattori di rischio che si annidavano nelle offerte più innovative (denominate commercialmente *flat*). Si sta attualmente lavorando per affinare un unico paradigma di intervento su queste criticità, che riguardano anche i versanti della telefonia fissa e della connettività wi -fi.

C'è da aspettarsi che la elaborazione dei modelli innovativi [14], attualmente sotto la lente del top management, andrà a costituire l'ossatura di uno strumento avanzato di *reporting*, capace di aggregare le informazioni e di fornire indicazioni essenziali per aggiornare con successo le policy di sicurezza e di prevenzione del rischio.

Bibliografia

[1] Davis S., Meyer C.: Blur, Olivares, 2002.

[2] Varian H., Farrell J., Shapiro C.: *Introduzione all'economia dell'informazione*. Etas, 2005.

[3] Beck U.: *Un mondo a rischio*. Einaudi, 2003.

[4] Mitnick K.: *L'arte dell'intrusione*. Feltrinelli, 2006.

[5] www.idc.com

[6] www.assinform.it

[7] Tagliapietra G.: *Etica della sicurezza*. In: Nova Review, dicembre 2006.

[8] Sofsky W.: *Rischio e sicurezza*. Einaudi, 2005.

[9] Prigogyne I.: *La fine delle certezze*. Bollati Boringhieri, 1997

[10] Telecom Italia. IT. *Security Report*, Vol. 5, 2005.

[11] Kelly K.: *Nuove regole per un mondo nuovo*. Ponte delle Grazie 1999.

[12] CSGE (a cura di): *Sicurezza: le nuove frontiere*. Franco Angeli, 2005.

[13] www.telecomitalia.it

[14] Chiesa R., Ciappi S.: *Profilo Hacker*. Apogeo, 2007.

Massimiliano Cannata è dottore in filosofia, giornalista professionista, autore televisivo e consulente d'impresa. Ha conseguito il *Master biennale Luiss in Giornalismo e Comunicazione d'Impresa*. Ha frequentato i corsi dell'*Ecole des Hautes Etudes* di Parigi e del Dipartimento di Linguistica dell'Università di *Paris VII*. Docente a contratto di *Storia della televisione e new media*, nell'ambito del Master in Storia, didattica e media, presso la Facoltà di Scienze Politiche dell'Università Statale di Milano. Collabora con vari periodici e riviste di cultura e divulgazione scientifica. Tra le ultime pubblicazioni: *Il viaggio delle idee. Per una governance dell'innovazione: intervista con Roberto Panzarani* (2005); *La sicurezza nell'era di Internet* (2005), *Formazione, competizione, innovazione, ricerca, rischio* (2004).
E-mail: maxcannata@yahoo.it

Maria Sabina Guerra si è laureata nel 2002 in Ingegneria Gestionale presso l'Università degli Studi della Calabria a Cosenza. Dal 2002 lavora in VP Tech, la BU Security di Value Team che si occupa di consulenza e soluzioni di sicurezza IT integrata. Dal 2003 opera come consulente per VPTech presso Telecom Italia in progetti correlati agli aspetti organizzativi e gestionali di sicurezza informatica e fornendo supporto nella definizione dei processi di security, policy e procedure in linea con gli adempimenti normativi. Per Telecom Italia cura inoltre alcune iniziative di security awareness e education.
E-mail: mariasabina.guerra@valueteam.com

Rocco Mammoliti ha studiato Ingegneria Elettronica a Pisa ed ha svolto per diversi anni attività di ricerca scientifica presso alcuni istituti del CNR (in particolare IEI, Istituto per l'Elaborazione delle Informazioni e IFC, Istituto di Fisiologia Clinica). È autore di diverse pubblicazioni scientifiche su temi legati alla modellistica e analisi statistica di dati e serie storiche, analisi di data mining e decision support system, sicurezza informatica, crittografia e data hiding. Ha svolto attività di consulenza e progettazione per diverse società nel settore informatico e delle telecomunicazioni. In particolare ha lavorato per Ericsson Telecomunicazioni, Engineering Ingegneria Informatica, Ernst & Young Consulting, Systeam, Bull Italia, Evidian. Dal 2002 lavora in Telecom Italia dove attualmente ricopre il ruolo di Responsabile della Funzione di Information Technology Security di Gruppo. È membro di alcune associazioni professionali internazionali tra cui l'IEEE (The Institute of Electrical and Electronics Engineers Inc., USA) e l'IEEE Computer Society.
E-mail: rocco.mammoliti@telecomitalia.it